

REMARKS

Claims 1-74 are pending in this application. Amendments to Claims 1-9, 14-15, 30-31, 42, 46, 51, 54, 59, 63, 65, and 70 are proposed herein. By these amendments, Applicants do not acquiesce to the propriety of any of Examiner's rejections. These amendments have been made solely to clarify the subject matter of the claims and no new matter has been added. These amendments, therefore, do not disclaim any subject matter to which the Applicants are entitled. *Cf. Warner Jenkinson Co. v. Hilton-Davis Chem. Co.*, 41 USPQ2d 1865 (U.S. 1997).

I. REJECTIONS UNDER 35 U.S.C. § 102

To properly maintain a rejection under 35 U.S.C. § 102, the Examiner must show that each and every limitation of the claims of the present invention is anticipated by the alleged prior art. *See In re Bond*, 15 USPQ2d 1896 (Fed. Cir. 1991). None of the cited references anticipate the present invention as claimed.

A. Rejection of claims 1-9, 54-58, and 70-74 under 35 U.S.C. § 102(e) as being anticipated by *Borza* (US 5,995,630)

As before, the Examiner rejected Applicants' claims 1-9, claims 54-58, and claims 70-74 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 5,995,630 issued to *Borza* ("*Borza*"). Office Action of September 16, 2005, page 2. Applicants respectfully traverse.

The present invention, in light of the proposed amendments to claims 1, 2, 54, and 70, is not anticipated by *Borza*. Specifically, *Borza* does not anticipate claims 1-9 because it does not disclose each and every element of those claims. The Examiner did not give "patentable weight" to the recitation "a remotely accessible secure cryptographic system...because the recitation occurs in the preamble" of claims 1-2. Office Action, pages 23-24. *Borza* relates to a device that includes both a user input and a cryptographic keys storage device in one single device; that is, the cryptographic key storage device is not remote from the user input. *Borza* at column 8, lines 30-36. Proposed amended claim 1 calls for a secure cryptographic system "wherein said secure cryptographic system is remotely accessible." Similarly. Proposed amended claim 2 calls for a secure cryptographic system "wherein said secure cryptographic system is remotely accessible." Therefore, *Borza* does

not anticipate claims 1-9 because it does not teach or disclose at least this element of those claims.

Furthermore, *Borza* does not anticipate claims 54-58 or claims 70-74 because it does not teach or disclose each and every element of those claims.

Proposed amended Claim 54 states:

A method of handling sensitive data from a plurality of users in a cryptographic system, wherein said sensitive data exists in a useable form only during actions employing said sensitive data, said method comprising:

- receiving in a software module, substantially randomized sensitive data portions from a first computer accessible storage medium;
- receiving in said software module, substantially randomized data portions from a second computer accessible storage medium,
- processing said substantially randomized sensitive data portions and said substantially randomized data portions in said software module to assemble said sensitive data; and
- employing said sensitive data in a software engine to [[said]] authenticate exactly one of said plurality of users.

Borza relates to “a method of analysing the biometric information” which is “characterised” where “[t]he characterisation produces numerical data...[and] an algorithm specific to this application is employed for generating data from the representation of the image.” *Borza* at column 7, lines 30-38. *Borza* also states, “the imaging device 120 provides data corresponding to a fingerprint to the comparator circuit 122...[which] compares the data with the biometric data previously stored in non-volatile memory.” *Borza* at column 8, lines 48-51.

Applicants respectfully disagree with the Examiner’s assertion that Applicants’ “randomized sensitive data” portions are akin to “the registered biometric data stored in the memory 123” of *Borza*. Office Action at page 6. Contrary to the Examiner’s comments, Applicants’ definition of substantially “randomized sensitive data” portions are not equivalent to *Borza*’s definition of “registered biometric data.” Applicants disclose “sensitive data, such as, for example, authentication data and the cryptographic key data.” Specification at page 28, lines 10-11. Applicants define in proposed amended claim 54 “processing the substantially *randomized sensitive data portions* and the substantially *randomized data portions* in the software module to assemble said *sensitive data*.” (Emphasis added).

Substantially randomized sensitive data portions and substantially randomized data portions are used to assemble “sensitive data, such as, for example, authentication data,” which includes, but is not limited to, “a user identification number, one or more biometrics, and a series of questions and answers generated by the trust engine 110 or the user, but answered initially by the user at enrollment.” *Id.* at page 12, lines 28-30.

Borza does not teach or disclose that registered biometric data is composed of “substantially randomized sensitive data portions from a first computer accessible storage medium” and “substantially randomized data portions from a second computer accessible storage medium.” (Emphasis added). Thus, *Borza* relates only to registered biometric data, not “substantially randomized sensitive data portions from a first computer accessible storage medium” and “substantially randomized data from a second computer accessible storage medium” used in “processing the substantially *randomized sensitive data* and the substantially *randomized data* in the software module to assemble said *sensitive data*.” (Emphasis added). Therefore, *Borza* does not anticipate claims 54-58 because it does not teach or disclose at least these elements of those claims.

Similarly, proposed amended claim 70 states:

A method of handling sensitive data in a cryptographic system, wherein said sensitive data exists in a useable form only during actions employing said sensitive data, said method comprising:

- receiving in a software module, substantially randomized sensitive data portions from a first computer accessible storage medium;
- receiving in said software module, substantially randomized data portions from a second computer accessible storage medium,
- processing said substantially randomized sensitive data portions from said first computer accessible storage medium and said substantially randomized data portions from said second computer accessible storage medium in said software module to assemble said sensitive data; and
- employing said sensitive data in a software engine to perform a cryptographic function.

Again, Applicants respectfully disagree with the Examiner’s assertion that Applicants’ “randomized sensitive data” portions are akin to “the registered biometric data stored in the memory 123” discussed in *Borza*. Office Action at page 6. Contrary to the Examiner’s comments, Applicants’ definition of substantially “randomized sensitive data”

portions are not equivalent to *Borza*'s definition of "registered biometric data." Applicants disclose "sensitive data, such as, for example, authentication data and the cryptographic key data." Specification at page 28, lines 10-11. Applicants define in proposed amended claim 70 "processing the substantially *randomized sensitive data portions* from said first computer accessible storage medium and the substantially *randomized data portions* from said second computer accessible storage medium in said software module to assemble said *sensitive data*." (Emphasis added). Substantially randomized sensitive data portions and substantially randomized data portions are used to assemble "sensitive data, such as, for example, authentication data," which includes, but is not limited to, "a user identification number, one or more biometrics, and a series of questions and answers generated by the trust engine 110 or the user, but answered initially by the user at enrollment." *Id.* at page 12, lines 28-30.

Borza does not teach or disclose that registered biometric data is composed of "substantially randomized sensitive data portions from a first computer accessible storage medium" and "substantially randomized data portions from a second computer accessible storage medium." (Emphasis added). Thus, *Borza* relates only to registered biometric data, not "substantially randomized sensitive data portions from a first computer accessible storage medium" and "substantially randomized data from a second computer accessible storage medium" used in "processing the substantially *randomized sensitive data* from said first computer accessible storage medium and the substantially *randomized data* from said second computer accessible storage medium in said software module to assemble said *sensitive data*." (Emphasis added). Therefore, *Borza* does not anticipate claims 70-74 because it does not teach or disclose at least these elements of those claims.

B. Rejection of claims 10-53 under 35 U.S.C. § 102(e) as being anticipated by Epstein (US 6,453,416)

The Examiner rejected claims 10-53 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,453,416 issued to Epstein ("*Epstein*"). Office Action at page 9. Applicants respectfully traverse.

Epstein does not anticipate the claims of the present invention. *Epstein* does not anticipate claims 10-13 because it does not teach "associating a user" with one or more "private cryptographic keys on a secure server." The Examiner argues that the "storing [of] either the private or the public key at the server is inherent" in *Epstein*. *Id.* at page 24. This

argument, however, does not lead to the conclusion that the private cryptographic key is inherently stored on the server.

“To establish inherency, the extrinsic evidence ‘must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.’ ” *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999) (citations omitted). “In relying upon the theory of inherency, the examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art.” *Ex parte Levy*, 17 USPQ2d 1461, 1464 (Bd. Pat. App. & Inter. 1990) (Emphasis in original).

The Examiner states that “storing either the private or the public key at the server is inherent,” and thus admits that the private cryptographic key is not necessarily stored at the server. In fact, *Epstein* distinctly shows at least one instance where the private key is not stored at the server when it states that the “[s]martcard also includes a memory for storing ... the user’s private key...” *Epstein* at column 5, lines 63-66.

Respectfully, Applicants assert that the Examiner’s use of *In re Casey*, 370 F.2d 576, 152 USPQ 235 (CCPA 1967), and *In re Otto*, 312 F.2d 937, 939, 136 USPQ 458, 459 (CCPA 1963), is inapposite to the method of claims 10-13. *In re Casey* and *In re Otto* relate to the germaneness of the manner or method in which a machine is to be utilized to the issue of patentability of the machine itself. *In re Casey*, 370 F.2d at 580. Claims 10-13 do not recite apparatuses; therefore, *In re Casey* and *In re Otto* are irrelevant.

In addition, *Epstein* does not anticipate claims 14-35 because *Epstein* does not teach each and every element of those claims. For example, *Epstein* relates to a “server 14 compris[ing] a memory 146” which “contains fields in a data structure, for storing user IDs, public keys, documents, and associated digital signatures DS, respectively for all users, which are indexed or otherwise addressable or retrievable by ID.” *Epstein* does not teach either “data splitting” or “data assembling” of “substantially randomized data portions of at least one enrollment authorization datum from enrollment authentication data” or “substantially randomized data portions of at least one cryptographic key from a plurality of cryptographic keys.” Therefore, *Epstein* does not anticipate claims 14-35 because it does not teach or disclose at least these elements of claims 14-35.

Epstein also does not anticipate claim 36. *Epstein* states that the “second data item I_2 is formed at block 62 by foreground process 124 hashing together document hash H_0 , random number RN and user identifying data U to a fixed length of at least 128 bits (160 bits if SHA-1 is used). also the first data item I_1 , is formed at block 64, which may occur earlier than as shown, by encrypting document hash H_0 using the public key of the user.” *Epstein* at column 7, lines 18-24. *Epstein* relates only to the use of a single random number RN throughout the patent with random number RN used exclusively to form only I_2 in a less complex combination.

In contrast, claim 36 claims “combining at said trust engine said authentication data with a first substantially random value to form a first combined value” and “combining authentication data with the *second* substantially randomized value to form a second combined value” to create “a first pairing of the first substantially random value with the second combined value” and “a second pairing of the first substantially random value” with the first pairing stored “in a first secure data storage facility” and the second pairing stored “in a second secure data storage facility remote from the first secure data storage facility.” (Emphasis added). Therefore, *Epstein* does not anticipate claim 36 because it does not teach or disclose at least this limitation of claim 36.

Furthermore, *Epstein* does not anticipate claims 37-44. For example, *Epstein* relates to a first data item I_1 created “by encrypting document hash H_0 using the public key of the user” and a second data item I_2 created by “hashing together document hash H_0 , random number RN and user identifying data U to a fixed length of at least 128 bits.” *Epstein* does not teach “combining the authentication data with the first set of bits to form a second set of bits” and “combining the authentication data with a third set of bits to form the fourth set of bits” to create “a first pairing of said first set of bits with said third set of bits” and “a second pairing of said first set of bits with said fourth set of bits” with the first and second pairing being stored “in a first computer accessible storage medium” and “in a second computer accessible storage medium.” Therefore, *Epstein* does not anticipate claims 37-44 because *Epstein* does not teach or disclose at least these elements of claim 37-44.

Finally, *Epstein* does not anticipate claim 45-53 because *Epstein* does not teach each and every element of those claims. *Epstein* relates to only the use of a single random number RN throughout the patent with random number RN used exclusively to form only I_2 in a less complex combination. For instance, *Epstein* does not teach “creating a first pairing of said first substantially random value with said second combined value” or “creating a second

pairing of said first substantially random value with said *second* substantially random value.” (Emphasis added). Therefore, *Epstein* does not anticipate claim 45-53 because it does not teach or disclose at least these elements of those claims.

C. Rejection of claims 59-69 under 35 U.S.C. § 102(e) as being anticipated by Pang (US 6,446,204)

The Examiner rejected claims 59-69 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,446,204, issued to Pang *et al.* (*Pang*). Office Action, page 19. Applicants respectfully traverse this rejection.

Pang does not anticipate the claims of the present invention. Specifically, *Pang* does not anticipate claims 59-64 because *Pang* does not teach each and every element of those claims.

Proposed Amended Claim 59 states:

A secure authentication system, comprising:

a plurality of authentication engines, wherein each authentication engine receives substantially randomized data portions of at least one piece of enrollment authentication data which once assembled are designed to uniquely identify a user to a degree of certainty, each authentication engine receives current authentication data to compare to said assembled enrollment authentication data, and wherein each authentication engine determines an authentication result; and

a redundancy system which receives said authentication result of at least two of said authentication engines and determines whether said user has been uniquely identified.

Pang states, “authorization information typically consists of such items as a user’s name and a password, a particular IP address, and specific domain name or other information that can identify a particular user and/or machine attempting to access information.” *Pang* at column 1, lines 53-58. Applicant discloses “randomized sensitive data portions of at least one piece of enrollment authentication data,” a concept which is not disclosed in *Pang*’s definition of “authorization information.” *Pang* does not teach “a plurality of authentication engines, wherein each authentication engine receives substantially randomized data portions of at least one piece of enrollment authentication data which once assembled are designed to

uniquely identify a user to a degree of certainty....” Therefore, *Pang* does not anticipate claims 59-64 because it does not teach or disclose at least these limitations of those claims.

In addition, *Pang* does not anticipate claims 65-69 because *Pang* does not teach each and every element of those claims.

Proposed Amended Claim 65 states:

A trust engine system for facilitating authentication of a user, said trust engine system comprising:

a first trust engine comprising a first depository, wherein said first depository includes a computer accessible storage medium which stores substantially randomized data portions of at least one piece of enrollment authentication data from a plurality of enrollment authentication data;

a second trust engine located at a different geographic location than said first trust engine and comprising:

a second depository having a computer accessible storage medium which stores substantially randomized data portions of at least one piece of said enrollment authentication data,

an authentication engine communicating with said first and second depositories and which assembles at least two of said substantially randomized data portions of at least one piece of said enrollment authentication data into a usable form, and

a transaction engine communicating with said first and second depositories and said authentication engine,

wherein when said second trust engine is determined to be available to execute a transaction, said transaction engine receives enrollment authentication data from a user and forwards a request for substantially randomized data portions of at least one piece of enrollment authentication data to said first and second depositories, and wherein said authentication engine receives said enrollment authentication data from said transaction engine and the substantially randomized data portions of at least one piece of said enrollment authentication data from said first and second depositories, and determines an authentication result.

Pang states, "authorization information typically consists of such items as a user's name and a password, a particular IP address, and specific domain name or other information that can identify a particular user and/or machine attempting to access information." *Pang* at column 1, lines 53-58. Applicant discloses "substantially randomized data portions of at least one piece of enrollment authentication data," a concept which is not disclosed in *Pang*'s definition of "authorization information." *Pang* does not teach "an authentication engine communicating with said first and second depositories and which assembles at least two of said substantially randomized data portions of at least one piece of said enrollment authentication data into a usable form." Therefore, *Pang* does not anticipate claims 59-64 because it does not teach or disclose at least these limitations of those claims.

CONCLUSION

Applicants have properly stated, traversed, accommodated, or rendered moot each of the Examiner's grounds for rejection. Applicant submits that the present application is now in condition for allowance.

If the Examiner has any questions or believes further discussion will aid examination and advance prosecution of the application, a telephone call to the undersigned is invited. If there are any additional fees due in connection with the filing of this amendment, please charge the fees to undersigned's Deposit Account No. 50-1067. If any extensions or fees are not accounted for, such extension is requested and the associated fee should be charged to our deposit account.

Respectfully submitted,



Don J. Peltó
Reg. No. 33,754

December 15, 2005

Preston Gates Ellis & Rouvelas Meeds LLP
1735 New York Avenue, NW, Suite 500
Washington, DC 20006
Telephone: (202) 661-3710
Facsimile: (202) 331-1024